Evaluation Checklist: System Owner IT Security Responsibilities

The information system owner is the Commerce manager responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system, and may rely on the assistance and advice of the IT Security Officer and other IT staff in the implementation of security responsibilities.

This checklist provides system owners with a self-assessment tool, and their supervisors with a performance evaluation to, to evaluate the level of compliance with system owner's duties as established by the *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSPP), Section 2.1.9, as well as the additional sections of the ITSPP cited in the second column of the checklist.

This is an assessment of (name/operating unit/office)**:**		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started **2** = In Process **3** = In Place

Performance Levels:

1 System owner has comprehensive IT security policies in place
2 System owner has comprehensive IT security policies as well as detailed procedures in place
3 System owner has comprehensive IT security policies and detailed procedures in place that are fully implemented for the owner's system
4 System owner has fully implemented and tested comprehensive IT security policies and detailed procedures in place
5 System owner has fully implemented and tested comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

	System Owner Responsibilities	ITSSP References*	Status	Performance Level
1	Develop the IT system security plan, including the initial risk assessment;	4.3, 3		
2	Ensure the system is operated according to the agreed upon security requirements;			
3	Decide who has access to the system (and with what rights and privileges);			
4	Ensure users and support personnel receive the requisite security training;	15		
5	Inform key agency officials of the need to conduct a security C&A effort;	6		
6	Provide necessary system-related documentation to the certification agent;			
7	Take appropriate steps to update the risk assessment and to reduce or eliminate vulnerabilities after receiving the security assessment results from the certification agent;			
8	Assemble and submit the Security Accreditation Package to the authorizing official or their designated representative;	6.5.2, 6.2.5,		

* In addition to Section 2.1.9

System Owner Responsibilities		ITSSP References*	Status	Performance Level
9	Ensure the Security Accreditation Package includes IT system security plans and contingency plans for all systems under their responsibility, which document the business associations and dependencies of their system(s) (examine and document linked IT resources and flow of information);	4.3, 9		
10	Maintain the original Security Accreditation Package that has been used for the initial accreditation decision;	6.5.2, 6.7.1,		
11	Update the Security Accreditation Package and ensure re-accreditation as the system undergoes a significant change or at list every three years:	6.5.2		
12	Include security considerations in the procurement of system software, hardware, and support services, including system development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management).	5.4		
13	Ensure certification and accreditation of all systems under their responsibility including:			
	(a) Ensuring the security of data and application software residing on their system(s);			
	(b) Determining and implementing an appropriate level of security commensurate with the system impact level.	3.4.1		
14	Conduct annual self-assessments of system safeguards and program elements;	6.3.1		
15	Establish system-level plans of action and milestones (POA&Ms) and implement corrective actions in accordance with the DOC standard for POA&Ms;	Appendix E		
16	Grant individuals the fewest possible privileges necessary for job performance (any privileges not specifically granted are denied access) so that privileges are based on a legitimate need to have system access, and re-evaluated the access privileges annually, revoking access in a timely manner upon personnel transfer or termination;			
17	Establish appropriate rules of behavior for all systems that apply to all personnel managing; administering, or having access to the DOC IT system;	4.5		
18	Notify the responsible IT Security Officer of any suspected incidents in a timely manner, and assist in the investigation of incidents if necessary;			
19	Ensure IT system IT service contracts include provisions for necessary security;			
20	Ensure system's personnel are properly designated, monitored, and trained, including appointment, in writing of an individual to serve as the Information System Security Officer (ISSO), if appropriate (large complex systems may have greater need for an ISSO than might a small, simple system).	2.1.10		